STATE of ARIZONA

Government **I**nformation **T**echnology **A**gency	**Statewide** **STANDARD** **P800–S860 Rev 2.0**	**TITLE: Virus and Malicious Code Protection** **Effective Date: April 5, 2004**

1. AUTHORITY

The Government Information Technology Agency (GITA) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) A.R.S. § 41-3504(A (1))) including the adoption of statewide technical, coordination, and security standards (A.R.S. § 41-3504(A (1(a)))).

2. PURPOSE

The purpose of this standard is to establish statewide virus and malicious code protection requirements to safeguard networks, IT components, and critically sensitive information from software contaminants (see Attachment A).

3. SCOPE

This applies to all budget units. Budget unit is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches. A.R.S. § 41-3501(2).

The Budget Unit Chief Executive Officer (CEO), working in conjunction with the Budget Unit Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures (PSPs) within each budget unit.

4. STANDARD

In an effort to safeguard networks, IT components, and critically sensitive information from software contaminants, each budget unit shall:

4.1. Protect all workstations and servers with virus-scanning software that has “notify and clean” enabled by default and that prevents users from disabling it.

4.2. Ensure that all remote workstations and servers used by State employees, contractors, and third-party entities that access budget unit internal networks are protected with virus-scanning software equivalent to that used by the budget unit. Virus-scanning software shall be configured and kept current as defined in paragraph 4.3 and 4.4.

4.3. Configure virus-scanning software to:

- Regularly scan all files that are stored on directly attached storage devices to the workstation.
- Automatically scan any file that is accessed or copied onto a directly attached storage device from an external source including electronically via the Internet, floppy disks, CD-ROM, or another internal budget unit network.
- Automatically scan any file that is accessed or modified (create, open, move, copy, or run) by a workstation software application, whether deployed on the individual workstation device, host- or server-based, or Application Service Provider (ASP) based.

4.4. Designate and document individuals having the responsibility and accountability to:

- Configure and execute (automatic execution is recommended) the appropriate virus-scanning software on all network-attached (wired and wireless) workstations.
- Periodically scan all files that are stored on Network Attached Storage, Storage Area Networking Systems, or any other devices such as PCs, laptops, etc., that are directly attached to a network server.
- Update and apply (automatic update is recommended) virus-scanning software with the most current virus definitions and program updates on all network servers that provide virus-scanning services to network-attached (wired and wireless) workstations and on all portable and stand-alone workstations.
- Apply the most current and appropriate inoculants and patches for each virus or malicious code infection on all network servers that provide virus-scanning services to network-attached (wired and wireless) workstations and on all portable and stand-alone workstations.

4.5. Expressly prohibit disabling of virus-scanning software.

4.6. Scan all incoming email, including attachments, for the existence of virus or malicious code. Viruses and malicious code shall be contained and eradicated upon discovery.

4.7. Implement a procedure that provides employees and contractors with a clear process, including appropriate contact points, to address, resolve, and report virus or malicious code infections within the budget unit.

4.8. Report each virus or malicious code infection in accordance with *Statewide Standard P800-S855, Incident Response and Reporting*, to the Statewide Infrastructure Protection Center (SIPC), within one hour of the occurrence, utilizing the SIPC incident reporting form and procedure.

4.9. Implement protection techniques that guard against virus and malicious code and potential intrusion via the use of Instant Messaging (IM), peer-to-peer (P2P) file-sharing, and Internet Relay Chat (IRC). Most IM and IRC services have little or no installed security services and use proprietary protocols. P2P data-centered (sharing of data held on other users' systems) file-sharing software represents a method capable of introducing malicious software (malware), adware, and spyware to internal networks as well as potential access to data/information without proper account management, authentication and authorization

- IM and IRC services are considered a form of email and are therefore covered by *Statewide Policy P401, Email Use*, and *Statewide Policy P501, Internet Use*.
- IM and IRC client software shall, if available, have the file transfer virus-scanning option activated and shall use the same virus-scanning software already in use for the client workstation or device.
- P2P file-sharing, application-sharing, and white-boarding should be prohibited unless the session is securely encrypted in accordance with *Statewide Standard P800-S850, Encryption Technologies*, and approved by the budget unit.
- Budget units allowing the use of IM, P2P file-sharing, and IRC services should educate users, in accordance with *Statewide Standard P800-S895, Security Training and Awareness,* of the virus/malicious code and social engineering security risks involved and the means of mitigating those risks.
- IM and IRC messages and attachments typically bypass firewalls or gateways that scan for malicious content, therefore encryption, if available, should be used.

5. DEFINITIONS AND ABBREVIATIONS

Refer to the PSP Glossary of Terms located on the GITA website at http://www.azgita.gov/policies_standards/ for definitions and abbreviations.

6. REFERENCES

6.1. A. R. S. § 41-621 et seq., "Purchase of Insurance; coverage; limitations, exclusions; definitions."
6.2. A. R. S. § 41-1335 ((A (6 & 7))),"State Agency Information."
6.3. A. R. S. § 41-1339 (A),"Depository of State Archives."
6.4. A. R. S. § 41-1461, "Definitions."
6.5. A. R. S. § 41-1463, "Discrimination; unlawful practices; definition."
6.6. A. R. S. § 41-1492 et seq., "Prohibition of Discrimination by Public Entities."
6.7. A. R. S. § 41-2501 et seq., "Arizona Procurement Codes, Applicability."
6.8. A. R. S. § 41-3501, "Definitions."
6.9. A. R. S. § 41-3504, "Powers and Duties of the Agency."
6.10. A. R. S. § 41-3521, "Information Technology Authorization Committee; members; terms; duties; compensation; definition."

6.11. A. R. S. § 44-7041, “Governmental Electronic Records.”
6.12. Arizona Administrative Code, Title 2, Chapter 7, “Department of Administration Finance Division, Purchasing Office.”
6.13. Arizona Administrative Code, Title 2, Chapter 10, “Department of Administration Risk Management Section.”
6.14. Arizona Administrative Code, Title 2, Chapter 18, “Government Information Technology Agency.”
6.15. Statewide Policy P100, Information Technology.
6.16. Statewide Policy P401, Email Use.
6.17. Statewide Policy P501, Internet Use.
6.18. Statewide Policy P800, IT Security.
 6.18.1. Statewide Standard P800-S850, Encryption Technologies.
 6.18.2. Statewide Standard P800-S855, Incident Response and Reporting.
 6.18.3. Statewide Standard P800-S895, Security Training and Awareness.
6.19. State of Arizona Target Security Architecture, http://www.azgita.state.az.us/enterprise_architecture.

7. ATTACHMENTS

A. Examples of Virus and Malicious Code.

Attachment A. Examples of Virus and Malicious Code.

Boot Sector - These viruses infect the first sector of a diskette or hard disk, which contains the master boot record, and are launched when a computer initializes with an infected disk. If a computer is booted with an infected diskette, the infected sector is loaded into memory and writes itself to the master boot sector on the hard drive. The virus stays in memory and infects new diskettes when the operating system accesses a new diskette and infects the boot sector of that disk. A boot sector virus, unlike other forms of viruses, does not travel across a network.

File Infectors - A type of virus that attaches itself to executable files, such as files with the extension .COM, .EXE, .DLL, .OVR, or .OVL. When the file is run, the virus, which operates in memory, spreads by attaching itself to other executable files. These types of viruses usually cause problems on LAN servers that run local applications shared by multiple systems. Unlike boot sector viruses, they can travel via a network as e-mail attachments or via file transfers. Gateway-based antivirus products stop the spread of these network-transported viruses by intercepting them at the network perimeter.

Macro Viruses - The macro virus represents the second generation of virus threat and spreads by means of macro instructions that are found in office applications such as Microsoft Word or Excel spreadsheets. The macros are typically stored as part of a document and can be transported as attachments to e-mail messages. Any application that supports automatically executable macros is a potential carrier for macro viruses, and because of the increasing use of the Internet, macro viruses are becoming more and more problematic. When a file containing an infected macro is used, the infected file reproduces the virus into an application from which it will infect other Word or Excel files. These types of viruses are not detected by traditional scanning engines, but can be detected using a heuristics approach.

Stealth Viruses - Stealth viruses hide from both the operating system and antivirus software by residing in memory and intercepting attempts to use the operating system via system calls. The virus hides, from both users and the antivirus software, the changes it makes to file size, directory structure, and/or other operating system aspects. Stealth viruses must be detected while they are in memory. Once found, they must be disabled in memory before the disk-based components can be corrected.

Polymorphic Viruses - Polymorphic viruses are encrypted viruses that change their appearance with each infection. They are difficult to detect because they hide from the antivirus software. In addition, these types of viruses complicate the AV software procedure because they alter the encryption algorithm with each infection.

Multipartite Viruses - Multipartite viruses infect both boot sectors and executable files. They can combine some or all of the stealth techniques, along with polymorphism to prevent detection.

Worm - A type of malicious code that does not alter files like a virus but resides in a computer's memory and replicates itself throughout a network (including the Internet) without the user being aware. It consumes system resources and floods the network with excessive traffic, eventually overloading the system and disrupting service.

Trojan Horses - Although Trojan horses are an elementary form of malicious code, they are still very problematic, particularly with the growth in use of Microsoft ActiveX and Sun Java applets. Trojan horses are not really viruses because they do not propagate themselves. Rather, they attack specific computers by enticing unsuspecting users into executing a command that appears benign. These commands can include seemingly innocent activities, such as initiating a screen saver, accessing an e-mail attachment, or downloading executable files from an untrusted Web site, which can then execute commands to destroy files or to give a hacker access to system files. When a file containing an infected macro is used, the infected file reproduces the virus into files or to give a hacker access to important system files. Although the Trojan horse does not inherently self-replicate, the introduction of and increase in use of Microsoft ActiveX control and Sun Java applet technology has increased the opportunity for Trojan horses to spread dramatically. Trojan horses can be used by hackers to enter the network, where upon they utilize Hypertext Transfer Protocol (HTTP) to establish communications.

Other types of Trojan horses can turn on a user’s camera or microphone and record conversations and retransmit them. Others are programs, such as Back Orifice, NetBus, or PrettyPark, which are marketed as legitimate software products with legitimate functions, but which can be used by hackers to penetrate a network. BackOrifice and NetBus are essentially remote administration tools that are installed as a server. A hacker with the corresponding client software can gain control of the system and eavesdrop, download files, or shut down the system. PrettyPark is spread as an e-mail attachment that logs users onto an Internet Relay Chat channel that can download passwords or credit card numbers.